AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

SHARON L. OVINGTON

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with DSID 1797954399, telephone number 937-543-1217, and the email address j.risner@live.com that is stored at Apple Inc.

Case No. 3:16mj-001

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
See Attachment A-2

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B-2

FILED
RICHARD W. NAGEL
CLERK OF COURT
2016 JAN -7 PM 2:31
U.S. DISTRICT COURT
SOUTHERN DIST. OHIO
DAYTON, OHIO

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
See Attachment C-2	

The application is based on these facts:
See Attached Affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Andrea R. Kinzig
Applicant's signature

Andrea R. Kinzig, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 1-7-16

Sharon L. Ovington
Judge's signature

City and state: Dayton, Ohio

Sharon L. Ovington, Chief U.S. Magistrate Judge
Printed name and title

ATTACHMENT A-2

Information associated with DSID **1797954399**, telephone number **937-543-1217**, and the email address **j.risner@live.com** that is stored at premises controlled by Apple Inc., a company that accepts service of legal process at 1 Infinite Loop, Cupertino, California, 95014.

ATTACHMENT B-2
Particular Things to be Seized

I. Information to be disclosed by Apple Inc. (the "Provider")

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-2:

a. Any device registration information, including customer name, address, email address, and telephone number.
b. Any customer service records, including: (1) records of support interactions with the customer regarding any Apple device or service, and (2) any device, warranty, and repair information.
c. Any information regarding any iTunes accounts, including: (1) subscriber information such as name, physical address, email address, and telephone number; and (2) information regarding iTunes purchase/download transactions and connections, update/re-download connections, and iTunes Match connections.
d. Any information regarding any iCloud accounts associated with the IMEI numbers, DSID numbers, email addresses, and telephone numbers identified in Attachment A-3, including (1) subscriber information such as name, physical address, email address, and telephone number; (2) mail logs, including records of incoming and outgoing communications such as time, date, sender email address, and recipient email address; (3) any available email content; (4) any other iCloud content, including photo streams, documents, contacts, calendars, bookmarks, and iOS device back-ups.
e. Any information regarding use of the Find My iPhone feature, including connection logs and transactional records.
f. Any available Game Center information, including connection logs with IP addresses and transactional records.
g. Any information regarding iOS device activations, including IP addresses of the events, ICCID numbers, and other device identifiers.
h. Any information available regarding any sign-on activity for iTunes, iCloud, and My Apple ID, including connection logs with IP addresses and transactional records.
i. Any information regarding My Apple ID and iForgot Logs, including connection logs with IP addresses and transactional records.
j. Any information regarding FaceTime communications, including call invitation logs.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of offenses involving violations of (1) possession of child pornography and access with intent to view child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) and 2252(a)(4)(B); (2) receipt and distribution of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) and 2252(a)(2)(B); (3) production of child pornography, in violation of 18 U.S.C. §§ 2251(a) and (e); and (4) coercion and enticement, in violation of 18 U.S.C. §2422, involving James Risner from August 11, 2013 to the present, including:

a. Any visual depictions and records related to the possession, receipt, and distribution of child pornography;

b. Any visual depictions of minors;

c. Any communications with others in which child exploitation materials and offenses are discussed and/or traded, and any contact / identifying information for these individuals;

d. Any communications with minors, and any contact / identifying information for these minors;

e. Evidence of utilization of email accounts, social media accounts, online chat programs, file storage accounts, including any account / user names;

f. Any information regarding utilization of websites and social media sites to access or obtain child pornography, communicate with juveniles, or communicate with others regarding child exploitation offenses;

g. Evidence of utilization of aliases and fictitious names;

h. Any information related to Internet Protocol (IP) addresses accessed by the account;

i. Information relating to who created, used, or communicated with the account, including records about their identities and whereabouts.

ATTACHMENT C-2

Code Section	Offense Description
18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2)	Possession of Child Pornography
18 U.S.C. §2252(a)(4)(B) & (b)(2)	Possession of Child Pornography
18 U.S.C. §2252(a)(2)(B) & (b)(1)	Distribution and Receipt of Child Pornography
18 U.S.C. §2252A(a)(2)(A) and (b)(1)	Distribution and Receipt of Child Pornography
18 U.S.C. §2251(a) & (e)	Production of Child Pornography
18 U.S.C. §2422(b)	Coercion and Enticement

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a), 2252A, and 2251) and offenses pertaining to coercion and enticement (in violation of 18 U.S.C. § 2422(b)). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media including computer media.

2. Along with other agents and officers of the Federal Bureau of Investigation and Clark County (Ohio) Sheriff's Office, I am currently involved in an investigation of the possession, distribution, receipt, and production of child pornography and coercion and enticement by JAMES EDWARD RISNER III (hereinafter referred to as JAMES RISNER). This Affidavit is submitted in support of Applications for search warrants for the following:

   a. Information associated with the email accounts **reset1888@gmail.com** and **jrisner82@gmail.com** that is stored at premises controlled by Google Inc. (as more fully described in Attachment A-1);

   b. Information associated with DSID **1797954399**, telephone number **937-543-1217**, and the email address **j.risner@live.com** that is stored at premises controlled by Apple Inc. (as more fully described in Attachment A-2);

   c. SanDisk for Wii 2 GB SD card, currently located at the Federal Bureau of Investigation, 7747 Clyo Road, Centerville, Ohio, 45459 (hereinafter referred to as the "**Subject Device**", and as more fully described in Attachment A-3).

3. The purpose of the Applications is to seize evidence of violations of 18 U.S.C. §§ 2252(a)(4)(B) and 2252A(a)(5)(B), which make it a crime to possess child pornography; violations of 18 U.S.C. §§ 2252(a)(2) and 2252A(a)(2), which make it a crime to receive and distribute child pornography through interstate commerce; violations of 18 U.S.C. §§ 2251(a) and (e), which make it a crime to produce child pornography; and violations of 18 U.S.C. § 2422(b), which make it a crime to use a facility of interstate commerce to coerce and entice another individual to engage in illegal sexual activities. The items to be searched for and seized are described more particularly in Attachment B-1 to B-3.

4. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other officers involved in the investigation. For purposes of

this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.

5. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support the searches of the above noted accounts and electronic device (as described in Attachments A-1 to A-3).

6. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of federal law, including 18 U.S.C. §§ 2251, 2252, 2252A, and 2422, are present within the information associated with the above noted accounts and electronic device (as described in Attachments A-1 to A-3).

JURISDICATION

7. This court has jurisdiction to issue the requested warrants because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND INFORMATION

Pertinent Federal Statutes

8. 18 U.S.C. § 2252(a)(4)(B) states that it is a violation for any person to knowingly possess, or knowingly possess with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

9. 18 U.S.C. § 2252A(a)(5)(B) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

10. 18 U.S.C. § 2252(a)(2)(B) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual

depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

11. 18 U.S.C. § 2252A(a)(2) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

12. 18 U.S.C. §§ 2251(a) and (e) states that it is a violation for any person to knowingly employ, use, persuade, induce, entice, or coerce any minor to engage in, or to have a minor assist any other person to engage in, or to transport any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, when he knew or had reason to know that such visual depiction would be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or attempts or conspires to do so.

13. For purposes of these statutes, the term "sexually explicit conduct" is defined in 18 U.S.C. § 2256(2) as:

a. "Actual or simulated –

i. Sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;
ii. Bestiality;
iii. Masturbation;
iv. Sadistic or masochistic abuse; or
v. Lascivious exhibition of genitals or pubic area of any person."

14. 18 U.S.C. § 2422(b) states that is a violation for any person to use the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States, to knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempt to do so.

Definitions

15. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

a. "**Child Pornography**" includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

b. "**Visual depictions**" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).

c. "**Minor**" means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).

d. "**Sexually explicit conduct**" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).

e. "**Internet Service Providers**" or "**ISPs**" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

f. An **Internet Protocol address**, also referred to as an **IP address**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as "octets," ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and

dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).

g. A network "**server**," also referred to as a "**host**," is a computer system that has been designated to run a specific server application or applications and provide requested services to a "client" computer. A server can be configured to provide a wide variety of services over a network, including functioning as a web server, mail server, database server, backup server, print server, FTP (File Transfer Protocol) server, DNS (Domain Name System) server, to name just a few.

h. A **client** is the counterpart of a server or host. A client is a computer system that accesses a remote service on another computer by some kind of network. Web browsers (like Internet Explorer or Safari) are clients that connect to web servers and retrieve web pages for display. E-mail clients (like Microsoft Outlook or Eudora) retrieve their e-mail from their Internet service provider's mail storage servers.

i. "**Domain Name**" refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top level domains are typically ".com" for commercial organizations, ".gov" for the governmental organizations, ".org" for organizations, and, ".edu" for educational organizations. Second level names will further identify the organization, for example "usdoj.gov" further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government. The Domain Name System, also referred to DNS, is a system of servers connected to each other using a common system of databases that resolve a particular domain name, such as "www.usdoj.gov," to its currently assigned IP address (*i.e.,* 149.101.1.32), to enable the follow of traffic across the Internet.

j. "**Log Files**" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

k. "**Hyperlink**" (often referred to simply as a "link") refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. "resource") to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.

l. "**Website**" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

m. "**Uniform Resource Locator**" or "**Universal Resource Locator**" or "**URL**" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

n. "**SD Card**" or a "**Secure Digital Card**" is a small flash memory card designed to provide high-capacity memory in a small size. SD cards are used in many small portable devices such as digital video camcorders, digital cameras, handheld computers, audio players, and mobile phones.

o. The terms "**records**," "**documents**," and "**materials**," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Characteristics of Collectors of Child Pornography

16. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter "collectors"):

a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.

b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion

collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.

c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.

d. Collectors almost always possess and maintain their "hard copies" of child pornographic images and reference materials (*e.g.,* mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector's residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years. Collectors often discard child pornography images only while "culling" their collections to improve their overall quality.

e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.

f. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during several recent nationwide law enforcement initiatives, including ICE's "Operation Emissary" and the FBI's "Ranchi message board" investigation. For example, in the "Ranchi" investigation a national take-down occurred during the week of March 1, 2007. Approximately 83 subjects were contacted, 28 by court-authorized search warrants and 55 by "knock and talks." Of the 83 contacts, 46 individuals (or 55%) confessed to accessing the Ranchi message board and/or downloading child pornography from Ranchi. Multiple other new cases were opened without confessions based on strong evidence obtained during the Ranchi search warrants and knock-and-talks.

Background on Google Inc.

17. Google Inc. is a multi-national corporation with its headquarters located in Mountain View, California. The company specializes in Internet-related products and services, including an Internet search engine (www.google.com), productivity tools such as email service (gmail), and enterprise products such as Google Search Appliance.

18. YouTube is a video-sharing website owned by Google, Inc., located at www.youtube.com. The website allows users to upload, view, and share videos. Most of the content on YouTube has been uploaded by individuals, although media corporations such as CBS and the BBC offer some of their material via the website. Unregistered users can watch the videos, but only registered users can upload videos. Registered users can also post comments about others' uploaded videos.

19. Google Photos is a free photograph and video sharing storage service, located at photos.google.com. It was launched by Google Inc. in May 2015. The service allows users to back-up their photographs and videos to a cloud service so that they are accessible by all devices connected to the service.

20. Google+ is a social networking and identity service website owned and operated by Google, Inc., located at www.plus.google.com. Common features include the following:

a. Profiles: Users can establish profile pages to maintain personal information, similar to the Facebook and MySpace social networking sites.

b. Circles: Google+ allows users to establish "circles", which enables them to organize people into groups for sharing across various Google products and services. This service replaces the typical "Friends" list function used by sites such as Facebook and MySpace.

c. Communities: Communities allow users with common interests to communicate with each other.

d. Photos: Google+ allows users to post, back-up, and share photographs. Users can also make comments on photographs posted by other users.

e. Hangouts: Hangouts are places used to facilitate group video chat. Only Google+ users can join such chats.

f. Messenger: Messenger is a feature available to Android, iPhone, and SMS devices for communicating through instant messaging within Circles.

21. Google Drive is a file storage and synchronization service provided by Google, Inc., located at www.drive.google.com. This service provides cloud storage[1], file sharing, and collaborative editing capabilities. It offers 15 GB of online storage space, which is usable across Google Drive, Gmail, and Picasa Web Albums.

Email Accounts

22. One of the services Google Inc. provides to users is electronic mail ("e-mail") access. Google allows subscribers to obtain e-mail accounts at the domain name gmail.com, like the accounts listed in Attachment A-1. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored

1 Cloud storage is a mechanism in which files can be saved to an off-site storage system maintained by a third party – i.e., files are saved to a remote database instead of the computer's hard drive. The Internet provides the connection between the computer and the database for saving and retrieving the files.

electronic communications (including retrieved and unretrieved e-mail for Google) and information concerning subscribers and their use of Google services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

23. A Google subscriber can also store with the provider files in addition to e-mails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to e-mails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

24. E-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

25. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

26. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

Apple Services and iPhones

27. Apple designs, manufactures, and markets mobile communication and media devices, personal computers, and portable digital music players, and sells a variety of related software, services, peripherals, networking solutions, and third-party digital content and applications. Apple's products and services include Mac, iPhone, iPad, iPod, Apple TV,

a portfolio of consumer and professional software applications, the iOS and Mac OS X operating systems, iCloud, and a variety of accessory, service and support offerings. Apple also sells and delivers digital content and applications through the iTunes Store, App Store, iBookstore, and Mac App Store.

28. The following represents a summary of some of the applications offered by Apple:

a. **iTunes** is a free software application which customers use to organize and play digital music and video on their computers. It also a store that provides content for customers to download for their computers and iOS devices. The iTunes Store is also available on the iPhone, iPad, and iPod Touch. Through the iTunes Store, users can purchase and download music, music videos, television shows, audio books, podcasts, movies, and movie rentals in some countries, and ringtones, available on the iPhone and iPod Touch (fourth generation onward). Application software for the iPhone, iPad and iPod Touch can be downloaded from the App Store.

b. **FaceTime** is a videotelephony[2] product. The video version of FaceTime supports any iOS device with a forward-facing camera and any Macintosh computer equipped with a FaceTime Camera, formerly known as an iSight Camera. FaceTime Audio is available on any iOS device that supports iOS 7 or newer, and any Macintosh with a forward-facing camera running Mac OS X 10.9.2 and later.

c. **iCloud** is a cloud storage and cloud computing service from Apple Inc. launched on October 12, 2011. The service provides its users with means to store data such as documents, photos, and music on remote servers for download to iOS, Macintosh or Windows devices; to share and send data to other users; and to manage their Apple devices if lost or stolen. The service also provides the means to wirelessly back up iOS devices directly to iCloud, instead of being reliant on manual backups. Service users are also able to share photos, music, and games instantly by linking accounts via AirDrop wireless. It replaced Apple's MobileMe service, acting as a data syncing center for email, contacts, calendars, bookmarks, notes, reminders (to-do lists), iWork documents, photos and other data.

d. **Game Center** is an online multiplayer social gaming network released by Apple. It allows users to invite friends to play a game, start a multiplayer game through matchmaking, track their achievements, and compare their high scores on a leader board.

29. According to Apple's Law Enforcement Guide, as published on its website, information maintained by Apple on its servers related to its products and applications includes the following:

a. Device Registration: Basic registration or customer information, including, name, address, email address, and telephone number, is provided to Apple by customers when registering an Apple device prior to iOS 8 and OS Yosemite 10.10. Apple does

---

2 Videotelephny is a means of simultaneous, two-way communication comprising of both audio and video elements. Participants in a video telephone communications can both see and hear each other in real time.

not verify this information, and it may not be accurate or reflect the device's owner. Registration information for devices running iOS 8 and later versions, as well as Macs running OS Yosemite 10.10 and later versions, is received when a customer associates a device to an iCloud Apple ID.

b. Customer Service Records: Contacts that customers have had with Apple's customer service regarding a device or service may be obtained from Apple. This information may include records of support interactions with customers regarding a particular Apple device or service. Additionally, information regarding the device, warranty, and repair may also be available.

c. iTunes: When a customer opens an iTunes account, basic subscriber information such as name, physical address, email address, and telephone number can be provided. Additionally, information regarding iTunes purchase/download transactions and connections, update/re-download connections, and iTunes Match connections may also be available.

d. iCloud: All iCloud content data stored by Apple is encrypted at the location of the server. When third-party vendors are used to store data, Apple never gives them the keys. Apple retains the encryption keys in its U.S. data centers. The following information may be available from iCloud:

i. Subscriber Information: When a customer sets up an iCloud account, basic subscriber information such as name, physical address, email address, and telephone number may be provided to Apple. Additionally, information regarding iCloud feature connections may also be available. Connection logs are retained up to 30 days.

ii. Mail Logs: Mail logs include records of incoming and outgoing communications such as time, date, sender email addresses, and recipient email addresses. iCloud mail logs are retained up to 60 days.

iii. Email Content: iCloud only stores the emails a subscriber has elected to maintain in the account while the subscriber's account remains active. Apple does not retain deleted content once it is cleared from Apple's servers. Apple is unable to provide deleted content.

iv. Other iCloud Content: Photo Stream, Docs, Contacts, Calendars, Bookmarks, and iOS Device Backups: iCloud only stores content for the services that the subscriber has elected to maintain in the account while the subscriber's account remains active. Apple does not retain deleted content once it is cleared from Apple's servers. iCloud content may include stored photos, documents, contacts, calendars, bookmarks and iOS device backups. iOS device backups may include photos and videos in the users' camera roll, device settings, app data, iMessage, SMS, and MMS messages and voicemail. iCloud content may be provided in response to a search warrant issued upon a showing of probable cause.

e. Game Center: Information regarding Game Center connections for a user or a device may be available. Connection logs with IP addresses, transactional records, and specific game(s) played may also be available.

f. iOS Device Activation: When a customer activates an iOS device or upgrades the software, certain information is provided to Apple from the service provider or from the device, depending on the event. IP addresses of the event, ICCID numbers, and other device identifiers may be available.

g. Apple Online Store Purchases: Apple maintains information regarding online purchases including name, shipping address, telephone number, email address, product purchased, purchase amount, and IP address of the purchase.

h. Find My iPhone: Find My iPhone is a user-enabled feature by which an iCloud subscriber is able to locate his/her lost or misplaced iPhone, iPad, iPod touch or Mac and/or take certain actions, including putting the device in lost mode, locking or wiping the device. Find My iPhone connection logs are available for a period of approximately 30 days. Find My iPhone transactional activity for requests to remotely lock or erase a device may be available

i. Sign-on Activity: Sign-on activity for a user or a device to Apple services such as iTunes, iCloud, My Apple ID, and Apple Discussions, when available, may be obtained from Apple.

30. My Apple ID: My Apple ID and iForgot logs for a user may be obtained from Apple. My Apple ID and iForgot logs may include information regarding password reset actions.

FACTS SUPPORTING PROBABLE CAUSE

Background of Investigation

31. In November 2015, an undercover task force officer of the FBI (hereinafter referred to as UCO-1), operating in the Washington, D.C. area, conducted an online investigation of individuals utilizing a file-sharing website to possess and distribute child pornography. This website will be referred to for purposes of this Affidavit as "Website A".

32. On or around November 23, 2015, UCO-1 located an account for an individual on Website A that had an album entitled "gymnastics daughter" and the following caption in the user profile: "email me for trade". The email address of reset1800@gmail.com was also listed on the profile page. The album contained various pictures of a pre-pubescent white female child with blonde hair wearing a gymnastics leotard. An adult white male was depicted in one of the photographs, although only the lower portion of his face was captured. The adult male was wearing a t-shirt with a logo for the Cincinnati Bengals (a football team in Cincinnati, Ohio).

33. Also on or around November 23, 2015, UCO-1 sent an email message to reset1800@gmail.com in which he identified himself as a "perv dad". The user of this email account quickly responded to UCO-1's message by stating "hi ok no prob s2r your dau pics only :)". Based on my training and experience, I know that "s2r" is a term to refer to "send to receive" and "dau" is short for "daughter". In my experience, I know that individuals involved in trading child pornography often request a new trading partner to send child pornography first to ensure that the new trading partner has files to share as well as to ensure that the new trading partner is not a law enforcement officer.

34. The reset1800@gmail.com account user continued to exchange messages with UCO-1 from approximately November 23, 2015 to November 26, 2015. Below is a summary of these messages:

a. The reset1800@gmail.com account user identified that the female child depicted in the photographs contained in the "gymnastics daughter" album was his daughter. The reset1800@gmail.com account user stated that his daughter was five years old at the time of the photographs but was currently seven years old.

b. In the exchange of messages, the reset1800@gmail.com account user asked UCO-1 if he was sexually active with his daughter. UCO-1 responded that he was, and the reset1800@gmail.com account user then stated: "yup same all the way round w/pics just don't have any of me doing her but i have. I already stole that cherry". Later in the exchange of messages, the reset1800@gmail.com account user stated: "Had to wait till she hit 7 to take her cherry to prevent tearing her and giving us away." Based on my training and experience, I believe that the reset1800@gmail.com account user was telling UCO-1 that he had vaginal sexual intercourse with his daughter on previous occasions but had not taken pictures of the sexual intercourse.

c. Also in the exchange of messages, the reset1800@gmail.com account user sent UCO-1 approximately five links to images on Yandex, a Russian website. The links contained at least approximately twenty-eight unique images of a pre-pubescent white female child that the reset1800@gmail.com account user indicated or specifically identified was his daughter. The images depict close-up images of the child's groin area and buttocks, some of which depict the child wearing white underwear and some of which depict her nude vagina and/or buttocks. None of the images depict the child's face. In some of the images, the child's finger(s) is (are) inserted in her vagina or spreading apart her vagina. Based on my training and experience, I believe that at least approximately nineteen of the images depict child pornography (as defined by 18 U.S.C. § 2256).

d. In approximately four of the images noted above, the child had a piece of paper in her hand with UCO-1's undercover name and the date of the email message (November 24, 2015). These images were sent in response to an inquiry made by UCO-1 if the reset1800@gmail.com account user actually had access to children. Based on my training and experience, I know that individuals involved in producing and trading child pornography sometimes include such papers in their images and videos as a means to validate that the files were recently produced. The files depicted close-up images of the pre-pubescent white female child's nude vagina. Based on my training and experience, I believe that two of the images depict child pornography (as defined by 18 U.S.C. § 2256). Given that the images contained the current date and the undercover officer's name, I believe that the images were produced on November 24, 2015.

e. The reset1800@gmail.com account user requested photographs of UCO-1's daughter on a number of occasions, often telling UCO-1 "s2r". The reset1800@gmail.com account user specifically requested nude photographs of UCO's daughter. For example, he stated: "To get mine i'm going to need some nudes :) All mine are!" The reset1800@gmail.com account user later again asked

UCO-1: "can u get me full nudes kinda like i got u?". Based on my training and experience, I believe that the reset1800@gmail.com account user was attempting to obtain child pornography from UCO-1.

f. Also in the messages exchanged with UCO-1, the reset1800@gmail.com account user discussed on several occasions efforts he took to conceal his identity. The reset1800@gmail.com account user stated that he utilized multiple email accounts as well as an "IP bouncer" to conceal his identity. When UCO-1 suggested that they chat via Kik (a cellular telephone based social media application), the reset1800@gmail.com account user responded: "not really i just don't trust anything that uses a cell phone. ALL CELL PHONES CAN BE TRACED! They can pull your text messages and calls also so they can intercept your images sent through kik that's why i don't use it. Even though it's kik it still uses a cell transmission or data connection to send and rec."

35. On November 27, 2015, the reset1800@gmail.com account user stated that he was changing his email account for "security reasons". He then exchanged emails with UCO-1 from the account child1st@yandex.com. In the exchange of messages, the child1st@yandex.com account user sent UCO-1 an email stating: "here's a link for you. Please view it quick. I'll have to destroy the images in the file so :/ gotta keep the gf happy". The email had a link to the Yandex file sharing website that contained approximately 15 image files. The child1st@yahndex.com account user told UCO-1 that the files were "recent". Based on my training and experience, I believe that all of the files depict child pornography (as defined by 18 U.S.C. § 2256). The images in summary depicted the following:

a. A pre-pubescent white female child who is completely naked and captured from the torso down, sitting on top of a naked adult white male (whose face is not captured).
b. What appears to be a child's hand touching an adult white male's penis.
c. What appears to be a white female child performing oral sex on an adult male's penis.
d. An adult white male's penis resting on or inserted into the vagina of a pre-pubescent white female child.
e. An adult white male secreting semen onto the vagina of a pre-pubescent white female child.
f. A pre-pubescent white female child spreading apart her vagina with her hands.
g. A blue couch was captured in the background of two of the images. The adult male was wearing a grey shirt in one of the images.

36. EXIF[3] data was available for approximately 26 of the images that the reset1800@gmail.com account user sent to UCO-1. The EXIF data identified that the

---

3EXIF is a format that is a standard for storing interchange information in digital photography image files using JPEG compression. Most new digital cameras use the EXIF annotation, storing information on the image such as shutter speed,

images were produced using a Fuji FinePix S8200 camera. EXIF data also identified that all of the images were created in January 2013. Based on my training and experience, I know that account creation dates produced in EXIF data can be inaccurate if the date and time settings on the camera are inaccurate, including if the settings are intentionally or unintentionally manipulated by the user. I also know that for some makes and models of cameras, date and time settings can be automatically reset when the batteries are removed from them.

37. Administrative subpoenas were served to Google requesting subscriber information and logs of IP addresses utilized to log into the account from the time period of November 1, 2015 to November 27, 2015 for the reset1800@gmail.com account. Records received by Google in response to the subpoena identified that the account was created on or about July 15, 2015, in the name of "afav bsdgafe". Based on my training and experience, I know that individuals involved in criminal activities often establish email, telephone, and other accounts in fictitious names in order to conceal their identities from law enforcement. The recovery4 email account identified for this account was rubmewrong18@hotmail.com. The log of IP addresses identified that the IP address of 174.101.208.24 was utilized on approximately 31 occasions to log into the account. A number of other IP addresses that appeared to be dynamic addresses were utilized on a number of occasions as well.

38. Records were requested from Time Warner Cable for subscriber information for the IP address of 174.101.208.24. Records from Time Warner Cable identified that the IP address was subscribed to in the name of The Wood Shop at 412 North Main Street, Suite 6, New Carlisle, Ohio (located in Clark County in the Southern District of Ohio); and with a contact telephone number of 937-679-5200. Records were also obtained from Time Warner Cable for a sample of the dynamic IP addresses that were utilized to log into the account on four separate dates in November 2015, most recently on November 27, 2015. Records from Time Warner Cable identified that each of these IP addresses was assigned to an account that was subscribed to in the name of JAMES RISNER, with a subscriber address of 217 Prentice Drive in New Carlisle, Ohio (also located in Clark County in the Southern District of Ohio) and contact telephone numbers of 937-679-5200 and 937-679-5326.

39. Internet searches for telephone number 937-679-5200 identified that the number was utilized by the business Rescue 1 Custom Vinyls, located at 412 North Main Street, Suite 5, New Carlisle, Ohio. The searches located a number of postings in which an adult female identified as Melissa Risner made comments about this business on the Facebook[5] website. In some of the postings, Melissa Risner identified that the business was owned by her husband, who was a firefighter. For example, on or about June 7, 2015, Melissa Risner posted the following message on a Facebook account in the name "Key West Fire

---

exposure compensation, F number, metering system used, if a flash was used, ISO number, date and time the image was taken, etc.

4 A recovery email account is an alternate email account that a user can establish that Microsoft can send the user's password to in the event that the user forgets his/her password.

5 The Facebook website (located at www.facebook.com) is a U.S.-based an online social networking website. Among other features, the website allows users to post pictures, videos, and comments and their accounts and communicate with others via a messenger application.

Station 1": "Hi, my husband is a firefighter in medway, ohio. Hehas opened a store in new Carlisle ohio and it is called rescue 1 custom vinyls. He is hoping to have a patch wall from fire departments all over the world. If you can halp me surprise him, by flooding his mailbox with patches that would be AMAZING!! His address is 412 N. Main Street, Suite 5, new Carlisle oh 45344 Thank you and god bless!!"

40. I have reviewed the property located at 412 North Main Street in New Carlisle, Ohio. I noted that the business contains seven business suites. Each suite has a glass storefront, allowing individuals to see inside the businesses. Written on the glass storefront of Suite 5 was the business name "Rescue 1" and the telephone number "679-5200". There were also writings on the glass indicating that the store sold window decals, vehicle decals, wall decals, vehicle wraps, banners, yard signs, and t-shirts. Seen in plain view inside Suite 5 was a computer monitor that appeared to be connected to a desktop computer tower. Suite 6 did not have any business names posted on its glass or door. However, there was a sign on the door for Suite 6 stating that the door was to be utilized only by Rescue 1 employees. There were also shirts hanging in the window that appeared to be merchandise for the Rescue 1 business. Seen in plain view inside the businesses was an interior open doorway that connected Suite 5 and Suite 6. Based on this information, I believe that Suite 5 and Suite 6 are both utilized by Rescue 1 Custom Vinyls.

41. Review of Melissa Risner's personal Facebook account as well as various other records checks indicate that Melissa Risner is married to JAMES RISNER. Review of JAMES RISNER's personal Facebook account indicates that he is employed as a firefighter. Review of postings on the Angie's List[6] website identified that the contact person for the Rescue 1 Custom Vinyls business was "Jim Risner".

42. As noted above, one of the photographs in the "gymnastics daughter" album depicted an adult white male, although his face was only captured from the nose down. Based on review of JAMES RISNER's driver's license photograph and photographs on his personal Facebook account, he strongly resembles the male in the photographs.

43. Photographs and the name of a young female child with blonde hair appeared on Melissa Risner's personal Facebook page. This child will be referred to for purposes of this Affidavit as "Minor Female A". Although she appeared older, Minor Female A resembled the child in the photographs in the "gymnastics daughter" album contained on Website A. As noted above, the reset1800@gmail.com account user identified that his daughter was five years old in these photographs but was currently seven years old. Records from the school that Minor Female A attends identified that she was seven years old, that Melissa Risner was her mother, and that she resided at 217 Prentice Drive in New Carlisle, Ohio. Because Minor Female A has a last name that appears to be Melissa Risner's maiden name or former last name, it is possible that Minor Female A is JAMES RISNER's step-daughter.

44. Based on records from the Ohio Bureau of Motor Vehicles, both JAMES RISNER and Melissa Risner utilize the address of 8945 East State Route 40 in New Carlisle, Ohio, on their current Ohio driver's licenses. Records from the Ohio Bureau of Motor Vehicles

---

6 The Angie's List website (located at www.angieslist.com) is a U.S.-based paid subscription website containing reviews of local businesses.

identified that JAMES RISNER and Melissa Risner have a 2005 Lincoln Navigator that is jointly registered to them. Although the address used on the registration paperwork was previously the 8945 East State Route 40 address, it was changed to 217 Prentice Drive in New Carlisle, Ohio in July 2015. However, this vehicle has been observed at the 8945 East State Route 40 address on a number of occasions during the time period of November 24, 2015 to November 27, 2015.

45. On November 27, 2015, a deputy of the Clark County Sheriff's Office went to 217 Prentice Drive in New Carlisle, Ohio to make a ruse contact with the occupants. Both JAMES RISNER and Melissa Risner were present at the house. JAMES RISNER confirmed that he owned Rescue 1 Custom Vinyls and would be at the business on the following Monday morning.

46. On November 28, 2015, federal search warrants were authorized by the United States District Court for the Southern District of Ohio for (1) the residential property located at 217 Prentice Drive, New Carlisle, Ohio, 45344, and (2) the business property located at 412 North Main Street, Suites 5 and 6, New Carlisle, Ohio, 45344. Agents and officers of the FBI and Clark County Sheriff's Office executed the warrants on November 29, 2015. Among other items, the following were seized:

a. Numerous desktop computers, laptop computers, and other electronic devices (seized from the residence and business);
b. Black Fuji FinePix S8200 camera, having a date set to January 1, 2013 (seized from the residence);
c. A toilet plunger with a wooden handle (seized from the business);
d. Blue couch cushion (seized from the residence).

47. JAMES RISNER was contacted and interviewed during the execution of the search warrants. After being advised of his Miranda Rights, JAMES RISNER provided the following information:

a. JAMES RISNER lived at 217 Prentice Drive along with his wife, Melissa Risner; his step-daughter, Minor Female A; and his five-year old son. They had resided at the residence since approximately June 2015. An adult male who will be referred to for purposes of this Affidavit as Adult Male A also previously lived at the residence from approximately June 2015 to November 25, 2015. Adult Male A was arrested on November 25, 2015, and has been in the custody of the Clark County Jail since that time.
b. JAMES RISNER was the owner of Rescue One Custom Vinyls. Both he and Melissa Risner regularly worked at the business. Adult Male A also worked at the business on a regular basis prior to his arrest.
c. JAMES RISNER and Melissa Risner received wireless Internet service through Time Warner Cable at both their residence and business. A password was required to access both accounts. Adult Male A as well as other friends knew the password for

the accounts. JAMES RISNER was not aware of anyone other than Melissa Risner and himself using his Internet service since the time of Adult Male A's arrest.

d. JAMES RISNER was shown two of the photographs from the "gymnastics daughter" album on Website A. JAMES RISNER identified that Minor Female A was depicted in both of the photographs, and that he was depicted in one of the photographs (the photograph of the adult white male wearing a Cincinnati Bengals shirt). JAMES RISNER stated that he had taken one of the photographs, and Melissa Risner had taken the other photograph. Minor Female A was approximately five years old at the time the photographs were taken. JAMES RISNER claimed that he had posted these and other similar photographs on the Facebook website at one time.

e. In addition to posting photographs of Minor Female A performing gymnastics on Facebook, JAMES RISNER and Melissa Risner also created and posted a video of Minor Female A performing gymnastics on the YouTube website on one occasion approximately two years ago. JAMES RISNER stated that he posted the video so that Melissa Risner's mother could see it. JAMES RISNER denied posting any other pictures or videos of Minor Female A performing gymnastics on any other websites.

f. JAMES RISNER advised that he and Melissa Risner had a black camera, the make and model of which he could not specifically recall. While Melissa Risner sometimes used it, JAMES RISNER was the primary user of the camera. He had taken pictures of Minor Female A with this camera on previous occasions. He typically uploaded the pictures from the camera onto a drive on his laptop computer.

g. JAMES RISNER identified that he utilized the email address j.risner@live.com.

h. JAMES RISNER stated that he did not currently have a cellular telephone.

i. JAMES RISNER denied any utilization of the email accounts reset1800@gmail.com or child1st@yandex.com. He also denied sending any pictures of Minor Female A to anyone via email. Shortly after being asked about the email accounts, JAMES RISNER terminated the interview.

48. Based on records from the Clark County Jail, I confirmed that Adult Male A has been incarcerated since November 25, 2015. As noted above, UCO-1 received email messages from the reset1800@gmail.com and child1st@yandex.com accounts after this date (specifically, on November 26, 2015 and November 27, 2015).

49. Melissa Risner was also interviewed during the execution of the search warrants. Below is a summary of information provided by Melissa Risner:

a. Melissa Risner reported information that was consistent with that provided by JAMES RISNER about the living arrangements and operation of the business.

b. Melissa Risner has never used or heard of the email addresses reset1800@gmail.com or child1st@yandex.com.

c. Melissa Risner was shown a sample of photographs that were sent to UCO-1 from the reset1800@gmail.com and child1st@yandex.com accounts. Melissa Risner provided the following information about these photographs:

i. Melissa Risner identified Minor Female A as being the individual in approximately six of the photographs based on the child's body parts, clothing, nail polish, scar, and/or other means. These photographs included one of the images that depicted a pre-pubescent white female child with a piece of paper in her hand with UCO-1's undercover name and the date of the email message (November 24, 2015). Melissa Risner recognized this photograph as being taken in the bathroom of the Rescue One Custom Vinyls business. Among other items, Melissa Risner recognized a wooden handle in the background of the image as being a plunger in the bathroom of the business. This handle is consistent with the plunger that was seized from the bathroom of the business during the execution of the search warrant (as detailed above).

ii. Melissa Risner recognized the clothing worn by the adult male in approximately two of the photographs to be JAMES RISNER's clothing.

iii. Melissa Risner recognized the furniture in approximately two of the photographs to be furniture in her residence.

50. On three occasions in November 2015 and December 2015, Minor Female A was interviewed by an individual who was trained in conducing forensic interviews of children. In summary, Minor Female A provided the following information during the two interviews:

a. Minor Female A identified that her father (JAMES RISNER) had taken photographs of what she referred to as her "cookie" (which she identified via an anatomical drawing as a vagina) on a number of occasions. On some occasions, he gave her notes to hold in her hand. These notes contained the names of the individuals to whom he was sending the pictures. On other occasions, JAMES RISNER told Minor Female A to put her finger inside her "cookie" and hold a note while he took the pictures. JAMES RISNER also took pictures of Minor Female A in her underwear and while she was performing gymnastics.

b. During the first interview, Minor Female A indicated that she had touched JAMES RISNER's penis with her hand but denied other types of sexual contact. During the second interview, Minor Female A disclosed that JAMES RISNER had vaginal and anal sexual intercourse with her, digitally penetrated her vagina, and performed oral sex on her. He also had her touch his penis and perform oral sex on his penis. These activities often happened at night after he woke her up from sleeping. JAMES RISNER had taken pictures and at least one video of some of these sexual activities.

c. The first occasion that JAMES RISNER had vaginal sexual intercourse with Minor Female A occurred when she was seven years old. This incident caused a significant amount of bleeding. JAMES RISNER instructed Minor Female A to say that the bleeding was the result of her putting her own fingers inside of her vagina. Minor Female A believed that all of the photographs were taken when she was seven years old.

d. Some of the photographs were taken at the Rescue 1 Custom Vinyls business, either in the bathroom or at JAMES RISNER's desk. Although she denied that pictures were taken at her residence during the first interview, Minor Female A identified in the second interview that a number of the pictures were also taken at her residence, including in her bedroom.

e. JAMES RISNER sent the pictures that he took of Minor Female A to others on the Internet, and these people sent JAMES RISNER pictures of what they did with their daughters.

f. The camera that JAMES RISNER used to take the pictures of Minor Female A had an "SD chip" in it. He downloaded the pictures onto his computer so that her mother would not find them.

g. JAMES RISNER showed Minor Female A child pornography on a number of occasions on two websites – Yandex and Website A. Minor Female A stated that JAMES RISNER's password on the Yandex website was "child1st". She also stated that JAMES RISNER had two email accounts that involved the phrase "child1st" – one that was a Google account and one that was a Yandex account.

h. During the two interviews, Minor Female A was shown a sample of photographs that were sent to UCO-1 from the reset1800@gmail.com and child1st@yandex.com accounts. Although she denied that she was the individual in some of the photographs during the first interview, Minor Female A positively identified herself as being the individual in approximately nineteen of the photographs during the second interview. Minor Female A identified that the photographs were taken at her residence or at the Rescue 1Custom Vinyls business. These photographs included the following:

i. Images of Minor Female A in her underwear;
ii. Close-up images of Minor Female A's vagina and/or buttocks;
iii. An image of Minor Female A with a piece of paper in her hand with UCO-1's undercover name and the date of the email message (November 24, 2015);
iv. An image of Minor Female A holding a card with "Chillover 99" written on it and touching her vagina;
v. Images of Minor Female A performing oral sex on JAMES RISNER's penis;
vi. Images of Minor Female A touching JAMES RISNER's penis;
vii. An image of JAMES RISNER secreting semen on Minor Female A's vagina;
viii. Images of JAMES RISNER engaging in vaginal sexual intercourse with JAMES RISNER.

i. JAMES RISNER told Minor Female A not to tell anyone about their sexual activities. JAMES RISNER told her that if she told anyone, he would go to jail for the rest of his life.

j. At the beginning of the second interview (prior to being shown the photographs), Minor Female A provided the interviewer with a crumpled orange post-it note. Minor Female A identified that this post-it name contained the names of individuals to whom JAMES RISNER sent photographs of her. Minor Female A stated that she found this note on her father's desk earlier that morning. One of the names written on the paper was "Chillover 99".

k. Minor Female A identified that JAMES RISNER had hit her on at least one occasion during the sexual activities.

51. During follow-up interviews, Melissa Risner identified that Minor Female A Minor Female A made statements indicating that JAMES RISNER began engaging in some of the sexual activities with her over a year ago. Melissa Risner also confirmed that there was an instance in which she found that Minor Female A was bleeding from her vagina, and that Minor Female A said that this was the result of touching her own vagina. Melissa Risner identified that this occurred in July 2015, shortly after Minor Female A's birthday party.

52. Based on my training and experience, I know that victims of child exploitation often do not fully disclose the extent of their sexual abuse during their first or subsequent interviews. Victims may not fully disclose the abuse due to feelings of embarrassment, feelings of affection toward their abusers, or threats made by their abusers, among other reasons. Also in my experience, I know that victims of child pornography offenses sometimes cannot or do not identify themselves in the photographs. Victims may not recognize or want to identify themselves due to feelings embarrassment, their lack of knowledge that the photographs were taken, or the limited focus of the images, among other reasons.

53. A preliminary examination has been conducted at this time of the SD card[7] contained in the Fuji FinePix S8200 camera that was seized from JAMES RISNER's residence pursuant to the search warrant. Recovered on the deleted space of this SD card were approximately six of the images that were sent to UCO-1 on November 27, 2015. Minor Female A also identified that she was the individual depicted in each of the images. The images depicted Minor Female A performing oral sex on JAMES RISNER, JAMES RISNER engaging in vaginal sexual intercourse with Minor Female A, and JAMES RISNER secreting semen on Minor Female A's vagina.

54. In reviewing the exterior of the Fuji FinePix S8200 camera, I noted that markings on the bottom of it identified that it was made in China. I therefore submit that the camera affects interstate or foreign commerce.

55. Based on all of the information noted above, I submit that there is probable cause to believe that JAMES RISNER is the user of the reset1800@gmail.com and child1st@yandex.com accounts. Furthermore, I submit that there is probable cause to believe that JAMES RISNER has produced, distributed, received, and possessed child pornography.

---

7 A Secure Digital card, commonly referred to as an SD card, is a type of memory card. It is often used to store images or data in digital cameras.

Email Account reset1888@gmail.com

56. In December 2015, records were obtained from Website A regarding the account that UCO-1 located when communicating with RISNER (the account containing the "gymnastics daughter" album, as detailed above). Records identified that two email addresses were associated with the account: reset1800@gmail.com and **reset1888@gmail.com**.

57. An administrative subpoena was served to Google Inc. requesting subscriber information and logs of IP addresses utilized to log into the account during the time period of January 1, 2015 to December 7, 2015 for the **reset1888@gmail.com** account. Records received from Google Inc. in response to the subpoena identified that the account was created on or around August 6, 2015 and was closed on or around September 2, 2015. Services available to the account included YouTube (among other services). The log of IP addresses identified that the IP address of 174.101.208.24 was utilized on approximately 87 occasions to log into the account. A number of other IP addresses that appeared to be dynamic addresses were utilized on a number of occasions as well. As noted above, records from Time Warner Cable identified that the IP address of 174.101.208.24 was assigned to an account for the Rescue One Custom Vinyls business and was also utilized on a number of occasions to access the reset1800@gmail.com account.

58. Based on information received from the subpoena served to Google Inc. as well as other information noted in the Affidavit, I believe that JAMES RISNER was the user of the **reset1888@gmail.com** email account. Although the account has been closed, a representative from Google Inc. informed me that content for closed email accounts may still be on Google Inc.'s servers if the subscriber did not delete the content prior to closing the account. Given JAMES RISNER's use of the reset1800@gmail.com and child1st@yandex.com accounts to receive and distribute child pornography and communicate about child exploitation activities, it is reasonable to believe that the **reset1888@gmail.com** account may also contain evidence of his child exploitation activities.

Email Account jrisner82@gmail.com

59. As detailed above, JAMES RISNER identified that he posted a video of Minor Female A performing gymnastics on the YouTube website. A search of the YouTube website located a video of Minor Female A performing gymnastics, posted by an account in the name of "Jim Risner".

60. An administrative subpoena was served to Google Inc. requesting subscriber information for the account that posted the video of Minor Female A performing gymnastics. Records received in response to the subpoena identified that the video was created by an account associated with the email address **jrisner82@gmail.com** on or around September 10, 2012.

61. An additional administrative subpoena was served to Google Inc. requesting subscriber information and logs of IP addresses utilized to log into the account during the time period of January 1, 2014 to December 20, 2015 for the **jrisner82@gmail.com** account.

Records received from Google in response to the subpoena identified that the account was created on or about March 1, 2012 in the name of "Jim Risner", and it was currently open. Services available to the account included YouTube, Google Photos, Google+, Google Drive, and YouTube (among other services). The log of IP addresses identified that the IP address of 174.101.208.24 was utilized on approximately 22 occasions to log into the account. A number of other IP addresses, some of which appeared to be dynamic addresses, were utilized to log into the account on a number of occasions as well. As noted above, records from Time Warner Cable identified that the IP address of 174.101.208.24 was assigned to an account for the Rescue One Custom Vinyls business and was also utilized on a number of occasions to access the reset1800@gmail.com and **reset1888@gmail.com** accounts.

62. Based on information received from the subpoena served to Google Inc. as well as other information noted in the Affidavit, I believe that JAMES RISNER is the user of the **jrisner82@gmail.com** email account. Given JAMES RISNER's use of the reset1800@gmail.com and child1st@yandex.com accounts to receive and distribute child pornography and communicate about child exploitation activities, it is reasonable to believe that the **jrisner82@gmail.com** account may also contain evidence of his child exploitation activities. It is also reasonable to believe that the YouTube account associated with this email address contains one or more videos that JAMES RISNER created of Minor Female A.

Apple iCloud Account

63. As noted above, JAMES RISNER stated during his interview that he did not have a cellular telephone. However, Melissa Risner identified that JAMES RISNER previously had an iPhone but had lost it a few weeks prior to the search warrant. Melissa Risner located this iPhone on or around December 6, 2015 and turned it over to investigators the following day. A search warrant was obtained from the United States District Court for the Southern District of Ohio authorizing the search of the iPhone. Subsequent search of the device identified that it was an iPhone 4 bearing serial number C8TKLJB3DP0V and telephone number **937-543-1029**. Based on review of the contents of the iPhone, I believe that it was previously utilized by JAMES RISNER.

64. As part of the investigation, an administrative subpoena was served to Apple Inc. requesting subscriber information, IP logs, transactional logs, and associated devices for any iCloud accounts associated with telephone number **937-543-1029**, the email address **j.risner@live.com**, and several other email addresses for the time period of January 1, 2014 to December 7, 2015. Apple provided records in response to the subpoena for on Apple device with the following device registration information:

a. iPhone 4 Black 8 GB bearing serial number C8TKLJB3DP0V: The device was purchased on or about August 11, 2013. Apple's records identified the device was registered to a customer with a name of James Risner; a street address of 8945 East State Route 40, New Carlisle, Ohio; and a telephone number of **937-543-1029**. The

account had an Apple logon ID of **j.risner@live.com**. The DSID[8] of **1797954399** was associated with the account.

65. Records provided by Apple identified that the DSID of **1797954399** was utilized to sign onto the following Apple services: FaceTime, Game Center, iCloud Account Services, and iTunes Music Store. Records indicated that the user signed up for the iCloud Account Services account on or around August 11, 2013, and last accessed the account on September 8, 2015.

66. Based on information received from the subpoena served to Apple Inc. as well as other information noted in the Affidavit, I believe that JAMES RISNER is the user of the Apple iCloud account associated with DSID **1797954399**, telephone number **937-543-1217**, and the email address **j.risner@live.com**.

Seizure of Subject Device

67. On January 5, 2016, I was contacted by Melissa Risner. Melissa Risner told me that she recently located the **Subject Device** inside a black case located in a plastic tote in her bedroom. Melissa Risner voluntarily turned over the **Subject Device** to me and provided her consent for officers to examine it.

68. The **Subject Device** is currently stored at the Federal Bureau of Investigation, and its electronic contents have not been accessed or examined by agents or other officers involved in the investigation. While the Federal Bureau of Investigation may have all necessary authority to examine the **Subject Device** based on Melissa Risner's consent, I seek this additional warrant out of an abundance of caution to be certain that an examination of the **Subject Device** will comply with the Fourth Amendment and other applicable laws.

Evidence Available in Email and Social Media Accounts

69. In my experience, individuals involved in child exploitation schemes often communicate with others involved in similar offenses about their victims and sexual activities via e-mail, social media accounts such as Google+, and online chat programs. I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.

70. Based on my training and experience, I know that individuals involved in child pornography offenses often trade images with each other via a variety of means, including email and social media accounts such as Google+. Such individuals may share images they have produced as well as images obtained from others. I have also seen a

8 A Destination Signaling Identifier (DSID) is a unique identification number assigned to each user when registering at iCloud.com.

number of cases in which individuals email files containing child pornography to themselves – either from one email account to another or from and to the same email account – in order to transfer the files from one electronic device to another.

71. Based on my training and experience, I know that individuals involved in child exploitation offenses often utilize multiple accounts, aliases, and means to communicate about child exploitation offenses and obtain child pornography. Multiple aliases are used as a means to avoid detection from law enforcement. Individuals also often attempt to obtain child pornography from a variety of sources, including those with whom they communicate via email; social media sites such as Google+; Internet chat programs; and on Internet bulletin boards; Internet Peer-to-Peer file sharing programs; Internet websites; and other sources. Evidence of multiple aliases, accounts, and sources of child pornography can often be found in the subjects' email and social media communications.

72. Most e-mail accounts have address books in which users can maintain names, e-mail addresses, and other information regarding individuals with whom they communicate. "Circles" and "Communities" in Google+ have similar names and information. This information can provide material evidence in cases involving sex trafficking offenses in that the information assists in identifying victims, co-conspirators, and clients.

73. Based on my training and experience, I know that many social media accounts and Internet websites require users to provide their email account when registering for the accounts. The social media account providers and Internet providers then send the users various notifications regarding messages from other users, information accessed by users, information available by the websites, and other information. These messages can provide material evidence in cases involving child exploitation offenses because they help in identifying what social media and Internet accounts were utilized by the subjects to communicate with other subjects and victims and what accounts were utilized by the subjects to find child pornography. In addition, the messages help in identifying the identities of other subjects and victims.

74. Also as noted above, social media and email providers maintain various subscriber and user information that its users provide when registering for its accounts. Such information is materially important in cases where social media and email accounts are utilized to trade child pornography, as this information can help in confirming the identity of the individuals using the accounts and committing the offenses.

75. Email and social media providers maintain various logs of IP addresses utilized to access the accounts. The IP information is again materially important in child pornography investigations. This information helps in identifying the subjects and the locations where their computer devices are located.

Evidence Available on Apple Inc. and Google Inc. Services

76. As detailed above in the Background section of the Affidavit, Apple's iCloud, Google Drive, and Google Photos are a cloud storage services that provide users with means to store files on remote servers. I also know, based on my training and experience, that individuals involved in child pornography offenses are increasingly utilizing cloud computing. Individuals with large collections of child pornography may utilize cloud

computing as a means to store their files after their hard drives become full. In addition, individuals utilize cloud computing as a means to conceal their files from others in the residence and/or from law enforcement. I have been involved in a number of prior investigations in which images and videos of child pornography were found in cloud storage accounts.

77. Again as detailed above in the Background section of the Affidavit, Apple's iCloud service also provides the means to wirelessly back up iOS devices directly to iCloud, instead of being reliant on manual backups. As such, data stored on cellular telephones can be recovered from the users' iCloud accounts. Therefore, the evidence detailed above that is commonly found on cellular telephones can also be found on the iCloud accounts.

78. Various other subscriber information, device activation information, sign-on logs, and transaction data are maintained by Apple for its products and applications. Such information is often materially relevant in child pornography investigations in that it helps in identifying the subjects and the locations where their computer devices are located.

79. As detailed above, the investigation identified that JAMES RISNER posted a number of photographs of Minor Female A in gymnastics clothing on Website A and discussed these images with those with whom he traded child pornography. The investigation also identified that JAMES RISNER posted at least one video of Minor Female A on the YouTube website. Based on my training and experience, I know that Google Inc. can search for, retrieve, and provide to investigators videos posted to YouTube by a particular account. Such videos may be materially relevant to the investigation of JAMES RISNER in that the videos can be compared to files posted to Website A and/or sent to other users via one of JAMES RISNER's email accounts.

Evidence Available on SD Cards

80. Based on my training and experience, I know that SD cards are commonly used in digital cameras to store pictures. I know that SD cards are often used to store images and other data from digital cameras. I also know that computer files and data can be stored on SD cards when they are plugged into computers through a card reader.

81. The **Subject Device** is marketed to be used in Wii gaming systems. However, I know based on my training and experience and from conducting Internet research that these SD cards are compatible with all devices with SD card slots, including digital cameras. As such, the **Subject Device** can be utilized to capture, store, and edit pictures.

82. Based on all of the information noted in the Affidavit, I believe that JAMES RISNER may have used the **Subject Device** to store child pornography.

ELECTRONIC COMMUNICATIONS PRIVACY ACT

83. I anticipate executing the warrants for the Google and Apple accounts under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrants to require Google and Apple to

disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachments B-1 and B-2. Upon receipt of the information described in Section I of Attachments B-1 and B-2, government-authorized persons will review that information to locate the items described in Section II of Attachments B-1 and B-2.

CONCLUSION

84. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the following criminal offenses may be located in the accounts and electronic device described in Attachments A-1 to A-3: (1) possession of child pornography and access with intent to view child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) and 2252(a)(4)(B); (2) receipt and distribution of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) and 2252(a)(2)(B); (3) production of child pornography, in violation of 18 U.S.C. §§ 2251(a) and (e); and (4) coercion and enticement, in violation of 18 U.S.C. §2422.

85. I, therefore, respectfully request that attached warrants be issued authorizing the search and seizure of the items listed in Attachments B-1 to B-3.

86. Because the warrants for the accounts described in Attachments A-1 and A-2 will be served on Google and Apple, who will then compile the requested records at times convenient to those entities, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

87. Because the warrants for the electronic device described in Attachment A-3 seek only permission to examine a device already in law enforcement's possession, the execution of the warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Special Agent Andrea R. Kinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 7th of January 2016

Sharon L. Ovington
Chief UNITED STATES MAGISTRATE JUDGE